UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/757,872	01/10/2001	John S. Flowers	22192-06893	8233

758 7590 05/04/2005

FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
TRAN, ELLEN C	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/757,872	FLOWERS ET AL.	
	Examiner	Art Unit	
	Ellen C Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 December 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 13-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 13-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/05, 1/05,& 8/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: 6 December 2004, the original application was filed on 10 January 2001 with a continuing application priority date of 10 January 2000.

2. Claims 1-10 and 13-29, are currently pending in this application. Claims 1, 8, 13, 17, 18, 21, 24, 25, and 27 are independent claims. Claims 11 and 12 have been cancelled. Claims 1, 2, 6, 7, 8, 13, 17, 18, 21, 24, 25, and 27 have been amended.

Response to Arguments

3. Applicant's arguments with respect to claims 1-8, 12-19, 23-30, 33-44, 47-50 have been considered but are not persuasive.

In response to applicant's argument on page 9, "These claimed rules allow an Intrusion Detection System (IDS) to detect and adapt to changes in the network environment without human intervention". The Office disagrees with argument; nowhere in the claims is the lack of human intervention claimed. In addition, although the applicant is arguing no human intervention takes place with the IDS. The specification indicates the IDS works with a VDS in which network conditions are checked against a rules database, that were constructed by an end user such as security or network engineer. Therefore the argument does not make sense. In Jerger a similar set of rules are defined by security zones which are set up by an end user for known security problems.

In response to applicant's argument on page 9, "Applicants respectfully submit that the method of Jerger fails to teach or disclose the claimed rules, which are determining the presence of a set of conditions in at least one network resource, wherein the set of conditions collectively define known network security properties of at least one network resource in which the set of

conditions are present". The Office disagrees Jerger defines properties of known security properties such as specific web sites or when downloading an active content from an un-trusted source.

In response to applicant' argument beginning on page 9, "In Jerger method, the security zones are predefined or configured by the user and the security configuration for each zone is also pre-configured as a set of security policy options ... By contrast, the claimed invention provides rules to determine the presence of condition in one network resource and the presence of those conditions reveal network security characteristics of that network resource that are generally known, e.g., "backdoors,"". The Office disagrees the claims as modified do not include any details that would overcome the Jerger reference. The modified claim text "for determining the presence of a set of condition in at least one network resource, wherein the set of conditions collectively define known network security properties of the at least one network resource in the set of conditions are present" has the same meaning as Jerger col. 3, lines 5-25 "the mechanism of the invention determines the security zone corresponding to the network location currently being browsed. Prior to performing a protected operation, the mechanism of the invention determines the action to perform, based on the current Web site's security zone, the requested operation, and the security setting corresponding to the requested operation and the Web site zone". Note "for determining the presence of a set of conditions" same as "determining the security zone" / "wherein the set of conditions collectively define known network security properties" same as "current Web site's security zone, the requested operation, and the security setting corresponding to the current Web site's security zone".

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

5. Claims 1-10 and 13-29, are rejected under 35 U.S.C. 102(e) as being anticipated by Jerger et al. U.S. Patent No. 6,473,800 (hereinafter '800).

As to independent claim 1, "A method for use in analyzing network security, comprising: constructing query-based rules for determining the presence of a set of conditions in at least one network resource, wherein the set of conditions collectively define known network security properties of the at least one network resource in which the set of conditions are present" is taught in '800 col. 3, lines 5-24.

As to dependent claim 2, "wherein network conditions include vulnerability conditions and intrusion conditions" is shown in '800 col. 3, lines 5-24.

As to dependent claim 3, "wherein the step of constricting query-based rules includes constructing query-based rules from a set of lexical elements that includes a set of templates" is disclosed in '800 col. 16, lines 26-56.

As to dependent claim 4 "wherein the templates are divided into two classes comprising template types and template actions" is taught in '800 col. 14, lines 49-67.

As to dependent claim 5, "wherein the step of constructing query based rules includes constructing query-based rules from a set of lexical elements that includes a set of statements, a set of templates, and a set of reserved words" is shown in '800 col. 16, line 57 through col. 17, line 6.

As to dependent claim 6, "wherein: known network security properties include vulnerability network security properties and intrusion network security properties; the set of statements includes SET and SELECT; the set of reserved words includes AND, TO, and WHERE; and the set of templates includes: a first subset of templates, the first subset of templates for determining the presence of conditions that collectively define known vulnerability network security properties, wherein the first subset comprises: Operating System, Host, Protocol, Application, Vulnerability, Port, Execute, ExecuteHex, Contains, and ContainsHex; a second subset of templates, the second subset of templates for determining the presence of conditions that collectively define known intrusion network security properties, wherein the second subset of templates comprises: Operating System, Protocol, Application, Port, Length, Offset, Threshold, Contains, ContainsHex, Flags, FragmentID, IcmpType, IcmpCode, PayloadSize, and TimeToLive" is disclosed in '800 col. 21, line 31-55 and col. 26, line 24 through col. 27, line 40.

As to dependent claim 7, "wherein the step of constructing query-based rules includes associating each rule with an operating system of at least one network resource" is taught in '800 col. 21, lines 31-55 and col. 26, line 24 through col. 27, line 40.

As to independent claim 8, A method for use in analyzing network security, comprising: constructing rules to be used for determining the presence of a set of

conditions in at least one network resource, wherein the set of conditions collectively define known network security properties of the at least one network resource in which the set of conditions are present, wherein the known network security properties include known vulnerability network security properties and known intrusion network security properties, the rules constructed from a set of lexical elements that include a set of templates, where each rule for identifying a vulnerability condition is associated with an operating system" is disclosed in '800 col. 3, lines 5-24

"from a set of lexical elements that include a set of templates, where each rule for identifying a vulnerability condition is associated with an operating system" is shown in '800 col. 21, lines 31-55, col. 26, line 24 through col. 27, line 40 and col. 14, lines 27-48 {Note, the security zone operates with the "system registry" which corresponds to the operating system of the security zone}..

As to dependent claims 9 and 10, these claims are substantially similar to claims 5 and 4; therefore they are rejected along the same rationale.

As to independent claims 13, this claim is directed to the system of the method of claim 8; therefore it is rejected along similar rationale.

As to dependent claim 14, this claim contains subject matter that is substantially similar to claims 1-6; therefore it is rejected along the same rationale.

As to dependent claim 15, "wherein: the rule constructor includes a graphical user interface to receive information from a user constructing a rule; and the rule, once constructed, is stored in a rule database" is taught in '800 col. 14, lines 33-48.

As to dependent claim 16, this claim contains subject matter that is substantially similar to claim 7; therefore it is rejected along the same rationale.

As to independent claim 17, this claim is directed to the system of the method in claims 1 and 2, therefore it is rejected along the same rationale.

As to independent claim 18, this claim is directed to the system of the method in claims 1-3; therefore it is rejected along the same rationale.

As to dependent claims 19-23, these claims contain subject matter that is substantially similar to claims 5-9; therefore they are rejected along the same rationale.

As to independent claim 24, "A system for use in network security, comprising: a rule constructor that allows a user to construct rules based on specified lexical elements" is taught in '800 col. 16, lines 26-56;

"where the rules are to be used for determining the presence of a set of condition in at least one network resource, wherein the set of conditions collectively define known network security properties of the at least one network resource in which the set of conditions are present" is shown in '800 col. 3, lines 5-24;

"a database for storing the rules" is disclosed in '800 col. 14, lines 33-48.;

"and an intrusion detector designed to monitor network traffic and to check that network traffic against the stored rules to determine if an intrusion exists on the network, the intrusion detector further designed to notify a user of the presence of an intrusion in at least one network resource, but only if the intrusion is applicable to the network resource based on the known intrusion properties of the network resource" is disclosed in col. 14, lines 49-67.

As to independent claim 25, this claim is directed to the system of the method in claim 11; therefore it is rejected along the same rationale.

As to independent claim 27, this claim is directed to the computer readable medium of the method in claim 11; therefore it is rejected along the same rationale.

As to dependent claim 26, 28, and 29, these claim contain subject matter that is substantially similar to claims 12 and 4; therefore they are rejected along the same rationale.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
11 April 2005

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER